VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Audit bezpečnosti informací

Information security audit

Student: Jiřina Petříková

Vedoucí práce: Ing. Martin Drastich, Ph.D.

Ostrava 2008

„Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracovala samostatně“

.....

Obsah:

Úvod

Bezpečnost informací je pojem, který stále více nabývá na významu. Příčinou je rostoucí cena informací, které znamenají pro mnohé firmy i existenční záležitost. Informace zprostředkovávají důležité obchody, zajišťují efektivnost práce, poukazují na nové možnosti v podnikání či rozvoji. Většina firem již vlastní nějakou formu informačního systému, který může být zneužit, poškozen, či napaden a je třeba jej chránit. Bez řádného zabezpečení totiž hrozí riziko úniku, poškození, či ztráty informací, což může mít za následek zhoršení konkurenceschopnosti firmy, ztrátu finančních prostředků nebo i poškození dobrého jména firmy, což by zkomplikovalo její další činnost.

V oblasti informační bezpečnosti figuruje mnoho standardů, podle nichž je možné bezpečnost daného systému posoudit. Rozsah zabezpečení je pro každou firmu individuální. Firmy s velkým počtem zákazníků mají jiné bezpečnostní požadavky než drobné firmy s malým obratem a nevelkou produkcí. Dalším kritériem je posouzení, jak velkou cenu mají interní informace v případě jejich ztráty. Pro některé firmy mají informace velmi vysokou cenu a investují do jejich ochrany nemalé prostředky.

První část bakalářské práce bude zaměřena na podrobnější charakteristiku bezpečnosti informaci a na audit IT. Dále zde budou uvedeny hlavní pojmy z těchto oblastí a jejich vymezení. V této části také provedu analýzu současného stavu firmy, na které bude audit aplikován.

Druhá část se bude věnovat analýze jednotlivých způsobů zabezpečení a posouzení jejich vhodnosti pro potřeby dané firmy. Cílem bude vybrat nejvhodnější způsob prověření zabezpečení.

Ve třetí části bude rozebrána příprava k provedení vlastního auditu podle vybraného standardu a jeho aplikace na danou firmu.

Cílem bakalářské práce je zhodnotit požadavky firmy a vybrat způsob zabezpečení, který nejlépe odpovídá potřebám dané firmy a následně podle tohoto standardu provést audit, který by měl upozornit na:

- možné zranitelnosti v informačním systému, které by mohly vést k jeho ohrožení;
- nedostatečnost ochrany ve vztahu k novým poznatkům v oblasti bezpečnosti IT;
- nedodržování vlastních bezpečnostních opatření.

1. Teoretická část – vymezení tématu, pojmy

1.1 Základní pojmy

1.1.1 Bezpečnost informací

Aktivum *(asset)*
cokoliv, co má pro organizaci hodnotu [ISO/IEC 13335-1:2004]

Dostupnost *(availability)*
zjištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby [ISO/IEC 13335-1:2004]

Důvěrnost *(confidentiality)*
zjištění, že informace jsou přístupné pouze těm, kteří jsou k přístupu oprávněni [ISO/IEC 13335-1:2004]

Bezpečnost informací *(information security)*
ochrana důvěrnosti, integrity a dostupnosti informací [ISO/IEC 17799:2005]

Událost v rámci systému managementu bezpečnosti informací *(information security event)*
identifikovaný výskyt stanu, indikujícího možné narušení nebo chybu zabezpečení, nebo předem neznámá situace, které mohou mít vliv na bezpečnost informací v rámci systému, služby nebo sítě [ISO/IEC TR 18044:2004]

Incident v rámci systému managementu bezpečnosti informací *(information security incident)*
jednotlivý nebo řada nechtěných nebo neočekávaných událostí souvisejících s bezpečností informací, s významnou pravděpodobností, že by mohly poškodit funkce organizace a ohrozit bezpečnost informací [ISO/IEC TR 18044:2004]

Systém managementu bezpečnosti informací *(ISMS – information security management system)*

část celkového systému managementu organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na vybudování, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací

Integrita *(integrity)*

zajištění správnosti a úplnosti informací a metod jejich zpracování [ISO/IEC 13335-1:2004]

Zbytkové riziko *(residual risk)*

riziko, které zůstává po ošetření rizik [ISO/IEC Guide 73:2002]

Akceptace rizika *(risk acceptance)*

rozhodnutí přijmout riziko [ISO Guide 73:2002]

Analýza rizik *(risk analysis)*

systematické používání informací k odhadu míry rizika a k určení jeho zdrojů [ISO Guide 73:2002]

Posuzování rizik *(risk assessment)*

celkový proces analýzy a hodnocení rizik [ISO Guide 73:2002]

Vyhodnocení rizik *(risk evaluation)*

proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu [ISO Guide 73:2002]

Management rizik *(risk management)*

koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika [ISO Guide 73:2002]

Zvládání rizik *(risk treatment)*

proces výběru a přijímání kontrol pro modifikaci rizika [ISO Guide 73:2002]

1.1.2 Audit IT

Audit *(audit)*
systematický, nezávislý a dokumentovaný proces získávání důkazů z auditu a jeho objektivního hodnocení s cílem stanovit rozsah splnění kritérií auditu [ISO 19011:2002]

Kritéria auditu *(audit criteria)*
soubor politik, postupů nebo požadavků [ISO 19011:2002]

Důkaz z auditu *(audit evidence)*
záznamy, konstatování skutečnosti nebo jiné informace, které souvisejí s kritérii auditu a jsou ověřitelné [ISO 19011:2002]

Zjištění z auditu *(audit findings)*
výsledky hodnocení shromážděných důkazů z auditu podle kritérií auditu [ISO 19011:2002]

Závěr z auditu *(audit conclusion)*
výstup z auditu poskytnutý týmem auditorů po zvážení cílů auditu a všech zjištění z auditu [ISO 19011:2002]

Klient auditu *(audit client)*
organizace nebo osoba žádající o audit [ISO 19011:2002]

Auditovaná organizace *(auditee)*
organizace, v níž se provádí audit [ISO 19011:2002]

Auditor *(auditor)*
osoba s odbornou způsobilostí k provádění auditu [ISO 19011:2002]

Tým auditorů *(audit team)*
jeden nebo více auditorů, kteří provádějí audit, a jsou podpořeni v případě potřeby technickými experty [ISO 19011:2002]

Technický expert *(technical expert)*

osoba, která poskytuje týmu auditorů specifické znalosti nebo odborné posudky [ISO 19011:2002]

Program auditů *(audit programme)*

jeden audit nebo soubor několika auditů naplánovaných pro určitý časový rámec a zaměřených na specifický účel [ISO 19011:2002]

Plán auditu *(audit plan)*

popis činností a uspořádání organizace auditu [ISO 19011:2002]

Předmět auditu *(audit scope)*

velikost a vymezení/ohraničení auditu [ISO 19011:2002]

Odborná způsobilost *(competence)*

prokázané osobní vlastnosti a prokázaná schopnost aplikovat znalosti a dovednosti [ISO 19011:2002]

1.2 Analýza současného stavu

1.2.1 Identifikace firmy

Firma Přeprava s. r. o. má sídlo v Ostravě a vlastní první patro soukromé budovy poblíž centra města. Do obchodního rejstříku byla zapsána v listopadu roku 2006 a vznikla za účelem distribuce komodity mateřské společnosti k zákazníkovi. Firma má 33 zaměstnanců a jako k právnické osobě se k ní vztahují zákony České republiky. Zároveň se řídí interními směrnicemi a příkazy, které jsou obsaženy v řídících dokumentech na intranetu společnosti. Jedná se o firmu, která má jediného společníka, a ten pověřil jejím vedením dva jednatele.

Jednatel je fyzická osoba, která je statutárním orgánem společnosti s ručením omezeným.

1.2.2 Technické a programové vybavení

Hardware

Počítačová síť je tvořena dvěma servery, které se nachází v pobočce mateřské společnosti v Brně. Společnost Přeprava s. r. o. má v provozu 23 počítačů a 10 notebooků značky Hewlett Packard, které jsou majetkem mateřské společnosti.

Ve firmě jsou dále k dispozici 2 laserové kopírky, 8 inkoustových tiskáren, 6 skartovacích zařízení a další příslušenství stejné značky.

Software

1) Důležité systémy:
   - Windows XP Professional Edition;
   - SAP R/3 („Systems - Applications - Products in data processing“);
   - Systémy na digitalizaci map;
   - Dispečerský systém.
2) Obecné kancelářské aplikace:
   - MS Internet Explorer 7 (internetový prohlížeč);
   - MS Outlook (poštovní klient);
   - MS Windows Player;
   - MS Office (kancelářský balík);
   - Adobe Reader (PDF prohlížeč);
   - 7 – Zip (souborový manažer a de/komprimátor).
3) Podpůrné kancelářské aplikace:
   - ASPIWIN;
   - BISW;
   - VPN Klient.

2. Standardy v oblasti informační bezpečnosti

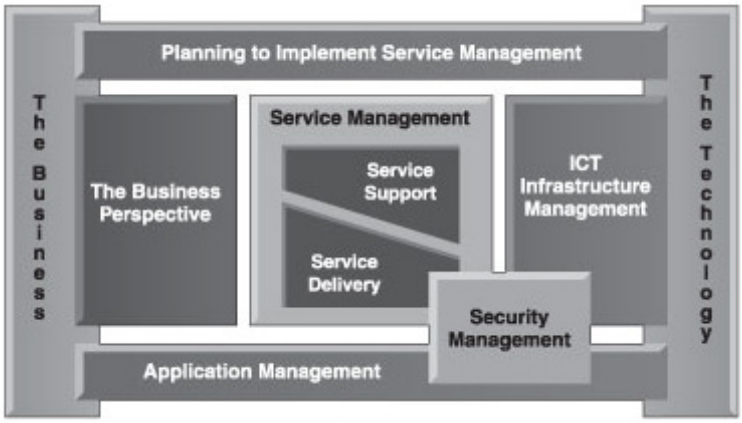
Existuje mnoho standardů, které se zabývají bezpečností informací. Každá firma si musí určit, jaké má požadavky na zabezpečení všech svých aktiv a podle toho zvolit nejvhodnější standard, který prověří jak její schopnost zabezpečit informace proti poškození, či zneužití, tak její konkurenceschopnost na trhu. Níže uvedené standardy jsou jedny z nejpoužívanějších v České republice. Každý z těchto způsobů zabezpečení má své charakteristické oblasti, které určují stupeň a rozsah zabezpečení systému řízení informační bezpečnosti.

2.1 Koncept ITIL

ITIL (*IT Infrastructure Library*) je rozsáhlý, procesně orientovaný rámec pro řízení IS/ICT služeb založený na "*best practices*". [6]

ITIL popisuje nejen procesy potřebné pro zajištění IT Service Managementu, ale také zásady jejich implementace, tj.:

- jednotlivé procesy a vzájemné vazby mezi nimi;
- cíle, vstupy, výstupy a dílčí aktivity jednotlivých procesů;
- role a odpovědnosti v jednotlivých procesech;
- způsoby měření kvality poskytovaných IS/ICT služeb a účinnosti jednotlivých procesů;
- kritické faktory úspěchu (CSF), potenciální problémy a možnosti jejich ošetření, atd.



Obr. 2.1 Základní struktura ITIL

Zdroj: http://modernirizeni.ihned.cz/c4-10065470-19237620-600000_d-kvalitativni-standardy-v-is-ict-cast-3-koncept-itil

Základní disciplíny resp. procesy IT Service Managementu v pojetí ITIL jsou:

a) Taktická úroveň *(Service Delivery)***:**

Service Level Management

Cílem tohoto procesu je vytvářet, udržovat a neustále zlepšovat kvalitu poskytovaných IS/ICT služeb a tím i vztahů se zákazníky.

Financial Management for IT Services

Cílem tohoto procesu je vykonávat nákladově efektivní správu IS/ICT aktiv a zdrojů, využívaných pro poskytování služeb.

Capacity Management

Má zaručit dostatek "nákladově ospravedlnitelných" IS/ICT kapacit pro naplňování současných i budoucích obchodních potřeb.

IT Service Continuity Management

Cílem tohoto procesu je zaručit kontinuitu obchodních aktivit organizace, které vyžadují IS/ICT zařízení, v souladu s požadovanými a odsouhlasenými časovými požadavky.

Availability Management

Má zaručit optimální dostupnost IS/ICT služeb dle požadavků "zákazníků" a za vynaložení přijatelných výdajů.

b) Operativní úroveň *(Service Support)***:**

Service Desk

Cílem tohoto procesu je umožnit kontakt se zákazníky a uživateli poskytovaných služeb, přijímat jejich požadavky týkající se poskytovaných služeb a zajistit jejich vyřízení. Sekundárně pak zajistit integraci a koordinaci dalších operačních procesů.

Incident Management

Zaměřuje se na obnovu normálního provozu poskytované služby, a to tak rychle, jak je to možné, za minimalizace dopadu na provoz obchodních procesů.

Problem Management

Směřuje k minimalizaci dopadu incidentů a problémů vzniklých v IS/ICT infrastruktuře na organizaci, resp. zabránění opakování incidentů.

Configuration Management

Cílem tohoto procesu je dokumentace a poskytování věrohodných informací o konfiguraci jednotlivých komponent IS/ICT infrastruktury ostatním procesům.

Change Management

Směřuje k minimalizaci nežádoucích dopadů na fungování a kvalitu IS/ICT služeb způsobených změnami v IS/ICT infrastruktuře.

Release Management

Má zaručit hladký a kontrolovaný průběh zprovoznění nových verzí SW a souvisejícího hardware.

2.2 Manažerský model COBIT

COBIT *(Control Objectives for Information and Related Technology)* je ucelený manažerský rámec a sada podpůrných nástrojů, který poskytuje souhrn osvědčených praktik napříč jednotlivými IS/ICT aktivitami a prezentuje aktivity v oblasti organizace a řízení IS/ICT v ucelené, logické struktuře.

COBIT se zaměřuje zejména do strategické oblasti organizace a řízení IS/ICT, je zaměřen více na řízení, než na vykonávání jednotlivých IS/ICT aktivit a je silně "obchodně orientovaný". Propojuje řízení IS/ICT s řízením organizace, je založený na procesním řízení, uplatňuje systematické metody monitorování a měření a je hierarchický. Základní princip COBITU spočívá v propojení tří základních oblastí: požadavků organizace, IS/ICT zdrojů a IS/ICT procesů. [7]

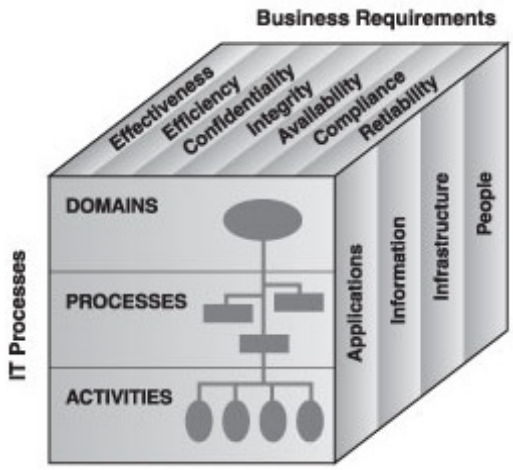
Definuje 34 procesů seskupených do 4 následujících domén:

- plánování a organizace;
- akvizice a implementace;
- poskytování a podpora;
- monitorování.

Pro každý proces jsou definovány:

- obsah a cíl;
- dílčí kontrolní cíle;
- typické aktivity a role;
- vstupy a výstupy;
- kritéria pro model vyspělosti;
- způsob měření;
- způsob auditu.

COBIT definuje a dále pracuje se sedmi kritérii informace: účinnost (*effectiveness*), efektivita (*efficiency*), důvěrnost (*confidentiality*), celistvost (*integrity*), dostupnost (*availability*), shoda (*compliance*), spolehlivost (*reliability*) a čtyřmi kategoriemi zdrojů: aplikace, informace, infrastruktura a lidské zdroje.



Obr. 2.2 COBIT kostka

Zdroj: http://modernirizeni.ihned.cz/2-19058910-600000_d-8c

COBIT se věnuje všem náležitostem řízení informatiky, zatímco ITIL je zaměřen na řízení ICT infrastruktury. COBIT a ITIL se navzájem nepopírají a naopak jsou do určité míry kompatibilní. COBIT má menší hloubku a současně širší zaměření než ITIL, který například neobsahuje řízení lidských zdrojů.

2.3 Norma ISO/IEC 27000

Tato mezinárodní norma je použitelná pro všechny typy organizací (např. komerční organizace, vládní organizace a úřady, neziskové organizace). Norma specifikuje požadavky na ustavení, zavedení, provoz, monitorování, udržování a zlepšování dokumentovaného ISMS v kontextu celkových rizik činností organizace. Specifikuje požadavky na zavedení bezpečnostních opatření, upravených podle potřeb jednotlivých organizací nebo jejich částí. [2]

Požadavky této normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. Vyloučení jakýchkoli požadavků je v případě, že chce organizace dosáhnout souladu s touto normou, nepřijatelné. [2]

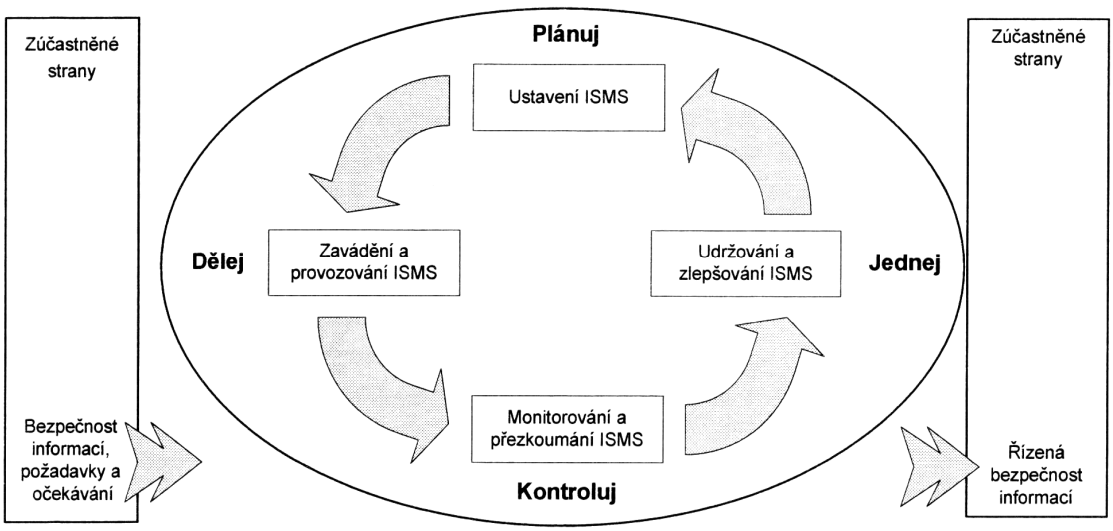
Podmínky normy:

- Vedení musí vyjádřit svůj závazek za dodržení podmínek normy.
- Organizace musí provádět pravidelné audity.
- Vedení organizace musí provádět přezkoumání ISMS v pravidelných intervalech.
- Organizace musí neustále zvyšovat účinnost ISMS

Aplikace systému procesů v organizaci, spolu s identifikací těchto procesů, jejich vzájemným působením a řízením může být označováno jako „procesní přístup“.

Při použití procesního přístupu pro management bezpečnosti informací tak, jak je prezentován v této normě, je kladen důraz na:

1. pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací;
2. zavedení a provozování opatření pro management bezpečnosti informací v kontextu s řízením celkových rizik činností organizace;
3. monitorování a přezkoumání výkonnosti a účinnosti ISMS;
4. neustálé zlepšování založené na objektivním měření.



Obr. 2.3 PDCA model aplikovaný na procesy ISMS

Zdroj: ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky : Systémy managementu bezpečnosti informací – Požadavky. 36 s.

2.4 Norma ISO/IEC 17799

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečnosti informací v organizaci. Cíle, popsané v normě, poskytují rady o obecně přijímaných cílech managementu bezpečnosti. [3]

Norma obsahuje celkem 11 základních oddílů, které jsou dále rozděleny do 39 kategorií bezpečnosti.

Oblasti bezpečnosti:

a) Bezpečnostní politika;

b) Organizace bezpečnosti;

c) Klasifikace a řízení aktiv;

d) Bezpečnost lidských zdrojů;

e) Fyzická bezpečnost a bezpečnost prostředí;

f) Řízení komunikací a řízení provozu;

g) Řízení přístupu;

h) Nákup, vývoj a údržba informačního systému;

i) Zvládání bezpečnostních incidentů;

j) Řízení kontinuity činností organizace;

k) Soulad s požadavky.

Každá z kategorií bezpečnosti obsahuje:

a) cíl opatření, určující čeho má být dosaženo;

b) jedno nebo více opatření, která lze použít k dosažení stanoveného cíle opatření.

Doporučení k realizaci poskytuje podrobnější informace a doporučení na podporu implementace vybraných opatření, která vedou k dosažení cíle opatření.

2.5 Vyhodnocení

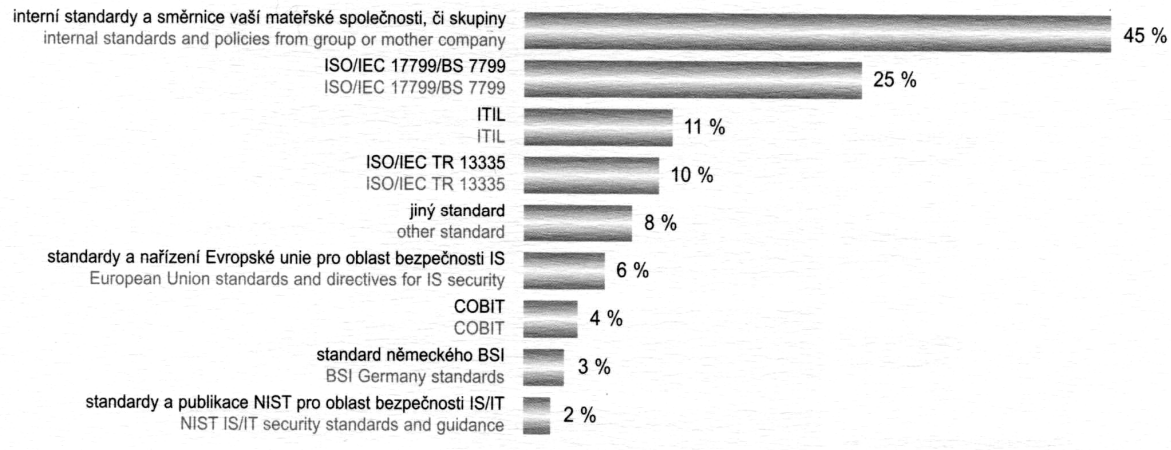
Komplexní ochrana informací je základem pro úspěšně splnění podmínek informační bezpečnosti a pro zajištění konkurenceschopnosti na trhu oproti „rizikovým" firmám. Získání některého z bezpečnostních standardů zhodnotí jméno společnosti a omezí ztráty v případě neočekávaných incidentů.

Systém bezpečnosti informací se skládá ze šesti základních oblastí:

- Fyzická bezpečnost;
- Režimová ochrana;
- Personální ochrana;
- Hardwarová ochrana;
- Softwarová ochrana;
- Ochrana informací v sítích.

Podcenění některého z těchto zabezpečení se promítne na celkovém zabezpečení informací v dané společnosti. Více než 40% firem v České republice uvádí, že k zajištění ochrany svých aktiv používají více než jeden standard. Jak je patrné z tab. 2.3, nejpoužívanější standardy v oblasti informační bezpečnosti jsou ISO/IEC 17799 a ISO/IEC 27000[1].

[1] ISO/IEC 27000 – aktuální norma vycházející z BS 7799



Obr. 2.4 Průzkum stavu informační bezpečnosti v ČR 2007

Zdroj: ERNST & YOUNG, NBÚ, DSM. Průzkum stavu informační bezpečnosti v ČR 2007. 28 s.[1]

Firma Doprava s.r.o. požaduje provedení auditu podle standardu, který zajišťuje komplexní přezkoumání zabezpečení všech oblastí firmy a který se řídí jasnými a závaznými pravidly pro kontrolu systému bezpečnosti. Po konzultaci s oprávněným zástupcem firmy jsem za standard k provedení auditu zvolila normu ISO/IEC 27000, která splňuje všechny uvedené požadavky. Tato norma je sice velmi podobná normě ISO/IEC 17799, ale liší se v přesně daných ustanoveních, které musí firma splňovat pro získání certifikátu bezpečnosti informací. Na rozdíl od konceptu ITIL se věnuje všem oblastem systému zabezpečení a oproti modelu COBIT neobsahuje žádná doporučení, ale přesně dané povinnosti pro splnění bezpečnostních kritérií.

[1] ERNST & YOUNG, NBÚ, DSM. *Průzkum stavu informační bezpečnosti v ČR 2007*. Praha : TATE International s.r.o., 2007. 28 s. ISBN 978-80-86813-13-4.

3. Praktická příprava a provedení vlastního auditu

3.1 Příprava auditu

Tato fáze zahrnuje předběžné přezkoumání dokumentace související s cílem, kritérii a rozsahem auditu, plán auditu a pracovní dokumenty.

Podle normy ISO/IEC 27000 jsem vypracovala otázky a vytvořila systém hodnocení jednotlivých otázek. Tento systém hodnocení má dva parametry:

- Míra splnění;
- Míra ověření.

Každý z těchto parametrů může nabývat tří hodnot:

- Písmeno A: Předmět otázky byl splněn, byl ověřen.
- Písmeno B: Předmět otázky nebyl zcela splněn, byl částečně ověřen.
- Písmeno C: Předmět otázky nebyl splněn, nebyl ověřen.

Pro hodnocení jednotlivých otázek jsem zvolila následující kritéria:

- 10 bodů: Předmět otázky je splněn a ověřen.
- 8 bodů: Předmět otázky je splněn a částečně ověřen.
- 6 bodů: Předmět otázky je splněn, ale není jej možno ověřit.
- 6 bodů: Předmět otázky není zcela splněn, ale je účinně ověřen.
- 4 body: Předmět otázky není zcela splněn a je částečně ověřen.
- 2 body: Předmět otázky není zcela splněn a není jej možno ověřit.
- 0 bodů: Předmět otázky není splněn.

Přehledně tento systém hodnocení zachycuje tab. 3.1.

Míra splnění	Míra ověření	Hodnocení
A	A	10 bodů
A	B	8 bodů
A	C	6 bodů
B	A	6 bodů
B	B	4 body
B	C	2 body
C	C	0 bodů

Tab. 3.1 Systém hodnocení otázek auditu

S oprávněnou osobou z firmy Doprava s.r.o. jsem upřesnila místo a čas konání auditu a zpracovala jsem plán auditu.

Plán auditu má být navržen tak, aby byl pružný a umožňoval změny s důrazem kladeným na informace shromážděné během auditu. Plán auditu byl sdělen všem zainteresovaným osobám.

Pomůckami k usnadnění šetření a k dokumentování zjištění z auditu mohou být kontrolní listy pro hodnocení specifických prvků, formuláře pro zaznamenávání zjištění z auditu nebo pro hodnocení procesu.

Výsledné hodnoty auditu budou dosazeny do vzorce (3.2), což je míra plnění, která se vypočítá jako procentní podíl dosaženého a maximálního počtu bodů ze všech otázek v dané kapitole. Suma těchto výsledků pak poslouží k výpočtu souhrnného hodnocení ISMS organizace pomocí vzorce (3.3).

$$M_n(PJ\text{-}nnn)^{1} = \frac{\text{Dosažený počet bodů ze všech otázek v dané kapitole}}{\text{Maximální možný počet bodů ze všech otázek v dané kapitole}} \times 100 \quad [\%] \qquad (3.2)$$

Zdroj: DRASTICH, M. Bezpečnost a ochrana dat a informací. 96 s.

$$H^{2} = \frac{\text{Suma míry plnění hodnocené kapitoly ISMS}}{\text{Počet hodnocených kapitol (prvků) ISMS}} \quad [\%] \qquad (3.3)$$

Zdroj: DRASTICH, M. Bezpečnost a ochrana dat a informací. 96 s.

[1] M_n (PJ–nnn) je míra plnění
[2] Souhrnné hodnocení

3.2 Provedení vlastního auditu

Pro audit bezpečnosti informací podle normy ISO/IEC 27000 jsem vypracovala následující otázky, které jsou rozčleněny do 13 kategorií. Každá kategorie představuje jeden prvek systému bezpečnosti informací. Hodnocení k těmto otázkám je obsaženo v příloze č. 1.

A Politika bezpečnosti informací

A.1 Máte dokument politiky bezpečnosti informací schválen vedoucími zaměstnanci?

A.2 Je zveřejněn a sdělen všem zaměstnancům?

A.3 Je sdělen partnerům?

A.4 Je politika bezpečnosti informací revidována v pravidelných intervalech a v případě podstatných změn pro zajištění kontinuální vhodnosti, přiměřenosti a účinnosti?

B Organizace bezpečnosti informací

B.1 Podporuje vedení aktivně bezpečnost informací?

B.2 Vyjádřilo vedení jasně svůj závazek a potvrdilo odpovědnost za bezpečnost informací?

B.3 Jsou aktivity pro zajištění bezpečnosti informací koordinovány představiteli z různých částí organizace?

B.4 Jsou určeny odpovědnosti za ochranu jednotlivých aktiv a za realizaci určených bezpečnostních procesů?

B.5 Máte určen postup schvalování nových prostředků pro zpracování informací z pozice managementu?

B.6 Máte identifikovány požadavky na důvěrnost nebo dohody o neprozrazení reflektující potřeby organizace ochránit své informace?

B.7 Jsou tato ujednání pravidelně přezkoumávána?

B.8 Udržujete příslušné kontakty s odpovídajícími autoritami (např. orgány státní správy)?

B.9 Udržujete příslušné kontakty s příslušnými zainteresovanými odbornými skupinami nebo jinými specializovanými bezpečnostními fóry a profesními sdruženími?

B.10 Přezkoumáváte přístup organizace k řízení bezpečnosti informací a jeho zavedení v pravidelných intervalech a při významných změnách, které mohou ovlivnit bezpečnost (tzn. cíle řízení, opatření, politiky, procesy a všechny postupy pro bezpečnost informací)?

C Externí partneři

C.1 Máte identifikována rizika, spojená s informacemi a zařízeními, fungujícími v rámci nakládání s informacemi, vznikající v procesech chodu podniku, do kterých jsou zapojeny třetí strany?

C.2 Máte přijata příslušná opatření ještě před udělením přístupových práv?

C.3 Zvažujete všechny identifikované bezpečnostní požadavky před zpřístupněním informačních aktiv nebo informací zákazníkovi?

C.4 Zohledňují smlouvy se třetími stranami, obsahující přístupy, činnosti, komunikování nebo řízení informací organizace nebo jejího zařízení pro nakládání s informacemi všechny příslušné požadavky na bezpečnost?

C.5 Zohledňují tyto požadavky také doplňující produkty nebo služby k zařízením pro zpracování informací?

D Řízení aktiv

D.1 Máte zavedenu evidenci všech důležitých aktiv spojených s informačními systémy?

D.2 Je tato evidence udržována?

D.3 Jsou všechny informace a aktiva spojená se zařízeními pro zpracování informací ve vlastnictví přesně označeného útvaru organizace?

D.4 Máte identifikována, dokumentována a zavedena pravidla pro přijatelné využívání informací a aktiv spojených se zařízením pro zpracování informací?

E Klasifikace informací

E.1 Jsou informace v organizaci klasifikovány podle svého významu, právních požadavků, citlivosti a významnosti pro organizaci?

E.2 Máte vymezen pro označování a zpracování informací přiměřený soubor postupů, které jsou ve shodě s klasifikačním schématem přijatým organizací?

F Bezpečnost lidských zdrojů

F.1 Máte stanoveny a dokumentovány bezpečnostní úlohy a odpovědnosti zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran v souladu s politikou bezpečnosti informací organizace?

F.2 Provádíte kontrolu a přezkoumání předchozích činností všech kandidátů na zaměstnání, smluvních dodavatelů a uživatelů z třetích stran podle příslušných zákonů a pravidel a úměrně požadavkům podniku?

F.3 Provádíte tuto kontrolu úměrně klasifikaci informací, se kterými mají nakládat a s nimi spojených rizik?

F.4 Musí zaměstnanci, smluvní dodavatelé a uživatelé z třetí strany při uzavírání pracovní smlouvy odsouhlasit a podepsat ustanovení týkající se odpovědnosti za bezpečnost informací jako součást svých podmínek pracovního poměru v pracovní smlouvě?

F.5 Vyžaduje management, aby zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran dodržovali bezpečnost podle vyhlášených politik a postupů organizace?

F.6 Musí zaměstnanci organizace, a je-li to důležité, i uživatelé třetích stran absolvovat odpovídající, pravidelně se opakující školení, vztahující se k politice bezpečnosti informací a postupům organizace?

F.7 Máte zaveden formalizovaný disciplinární proces pro zaměstnance, kteří ohrozili bezpečnostní rozhraní?

F.8 Máte jasně určeny a formulovány odpovědnosti při ukončování zaměstnaneckého poměru nebo při změně zaměstnání v rámci organizace?

F.9 Musí zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran před ukončením zaměstnání, smlouvy nebo dohody vrátit všechna aktiva, náležející organizaci, která spravovali při výkonu funkce?

F.10 Jsou přístupová práva všech zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran k informacím a zařízením pro zpracování informací odejmuta před ukončením jejich zaměstnanosti, smlouvy nebo dohody?

F.11 Jsou přístupová práva v případě změny včas aktualizována podle povahy změny?

G Fyzická bezpečnost a bezpečnost prostředí

G.1 Používáte při ochraně prostor, ve kterých se nachází zařízení pro zpracování informací, bezpečnostní perimetry (bariéry jako zdi, vstupy pomocí čipových karet, recepce apod.)?

G.2 Jsou bezpečné prostory chráněny vhodnými opatřeními, aby byl přístup povolen pouze oprávněným osobám?

G.3 Jsou vytvořeny zabezpečené oblasti pro ochranu kanceláří, místností a vybavení se zvláštními bezpečnostními požadavky?

G.4 Máte zavedenu fyzickou ochranu proti zničení požárem, povodní, zemětřesením, explozí a dalším živelným nebo společenským ohrožením?

G.5 Využíváte další opatření a směrnice pro zvýšení bezpečnosti v zabezpečených oblastech?

G.6 Máte pod dohledem přístupová místa, díky kterým by neautorizované osoby mohly vstoupit do prostorů organizace?

G.7 Pokud je to možné, jsou tato místa izolována od zařízení pro zpracování informací, aby nemohlo dojít k neautorizovanému přístupu?

G.8 Máte všechna zařízení umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím?

G.9 Máte bezpečnostní opatření k omezení příležitosti pro neoprávněný přístup k zařízením?

G.10 Jsou tato zařízení chráněna před selháním napájení a před dalšími formami přerušení, způsobenými poruchami podpůrných zařízení?

G.11 Je silová a telekomunikační kabeláž, určená pro přenos dat a podporu informačních služeb, chráněna před poškozením či odposlechem?

G.12 Jsou veškerá zařízení udržována v souladu s pokyny výrobce a s dokumentovanými postupy?

G.13 Jsou při ochraně zařízení, které je použito mimo objekty organizace, zohledněna různá rizika prací mimo prostory organizace?

G.14 Jsou všechny prvky zařízení, obsahujícího paměťová média, před tím, než se dají dále k dispozici, zkontrolovány, aby se zajistilo odstranění všech citlivých dat a softwarů?

G.15 Je možno odstranit vybavení, informace a software jen se schválením (autorizací)?

H Řízení telekomunikace a řízení provozu

H.1 Jsou provozní postupy dokumentovány, udržovány a k dispozici všem, kteří je potřebují?

H.2 Provádí se změny na zařízeních, využívaných pro práci s informacemi, řízeným způsobem?

H.3 Jsou povinnosti odděleny od oblastí odpovědnosti, aby se omezila příležitost neoprávněné nebo i neúmyslné modifikace nebo zneužití aktiv organizace?

H.4 Je od sebe odděleno vybavení pro vývoj, testování a provoz, aby se snížilo riziko neautorizovaného přístupu nebo změn v operačním systému?

H.5 Máte zajištěno, aby smlouvy se třetí stranou o dodávání služeb obsahovaly výčet opatření, přesná stanovení služeb a úrovně jejich dodávání?

H.6 Obsahují tyto smlouvy požadavek, aby třetí strany tato ustanovení průkazně dodržovaly?

H.7 Jsou služby, hlášení o jejich provádění a záznamy poskytované třetí straně pravidelně monitorovány a přezkoumávány (včetně pravidelného provádění auditů)?

H.8 Jsou změny v rámci poskytovaných služeb, včetně udržování a zlepšování existujících informačních politik, postupů a opatření řízeny?

H.9 Je v rámci provádění změn provedeno nové hodnocení rizik?

H.10 Je využívání zdrojů monitorováno a vylaďováno pro zajištění požadované výkonnosti systému?

H.11 Děláte prognózy požadavků na budoucí kapacity?

H.12 Máte určena kritéria pro akceptaci nových systémů, jejich aktualizaci a zavádění nových verzí?

H.13 Jsou tato kritéria podpořena vhodnými testy systému, které jsou prováděny před vlastní akceptací?

H.14 Máte implementována opatření pro odhalování, prevenci a znovunabytí ztracených dat, aby byla zajištěna ochrana před působením škodlivých programů a aby bylo zvyšováno odpovídající bezpečnostní povědomí uživatelů?

H.15 Máte zajištěno pomocí správného nastavení konfigurace, aby autorizovaný mobilní kód pracoval v souladu s jasně stanovenou bezpečnostní politikou a aby fungovala ochrana proti využívání neautorizovaného kódu? (Jen pokud je v organizaci povoleno využívání mobilních kódů)

H.16 Pořizujete pravidelně záložní kopie informací a programového vybavení podle odsouhlasené politiky pro zálohování?

H.17 Jsou tyto kopie pravidelně testovány?

H.18 Jsou sítě v organizaci přiměřeně kontrolovány a řízeny?

H.19 Jsou zvláštní požadavky na bezpečnost, úrovně služeb a požadavky na management všech síťových služeb správně identifikovány a zavedeny do všech smluv na síťové služby?

H.20 Existují postupy pro správu vyměnitelných počítačových médií?

H.21 Jsou média, která jsou dále provozně neupotřebitelná, bezpečně a spolehlivě zlikvidována dokladovanými postupy?

H.22 Jsou vytvořeny postupy pro nakládání s informacemi a jejich ukládání, které je chrání před neoprávněným využitím nebo prozrazením?

H.23 Je systémová dokumentace chráněna před neoprávněným přístupem?

H.24 Existují politiky, postupy a opatření pro ochranu výměny informací s použitím všech typů komunikačních zařízení?

H.25 Jsou mezi organizací a externími partnery uzavřeny dohody pro výměnu informací a programového vybavení?

H.26 Jsou média obsahující informace chráněna proti neautorizovanému přístupu, zneužití nebo poškození při transportu mimo organizaci?

H.27 Jsou informace přenášené elektronickou poštou vhodným způsobem chráněny?

H.28 Jsou vytvořeny a zavedeny politiky a postupy pro ochranu informací souvisejících s propojením obchodních informačních systémů?

H.29 Jsou informace z elektronického obchodování, které procházejí přes veřejné sítě, ochráněny od podvodných aktivit, nedorozumění ve smlouvách a neoprávněných odhaleních a modifikacích?

H.30 Jsou informace týkající se obchodů uzavíraných on-line chráněny, aby se zabránilo neúplnému přenosu, chybnému směrování, neoprávněné úpravě, neoprávněnému odhalení, neoprávněnému zdvojení nebo modifikaci?

H.31 Je chráněna celistvost informací, které jsou k dispozici na veřejně přístupných systémech, aby nemohlo dojít k neoprávněné modifikaci?

H.32 Jsou auditní logy, zaznamenávající aktivity uživatelů, výjimky a události související s bezpečností informací udržovány po stanovenou dobu pro účely možných budoucích vyšetřování a monitorování řízení přístupů?

H.33 Máte určeny postupy pro monitorování využití zařízení pro zpracování informací?

H.34 Jsou výsledky z těchto zařízení pravidelně vyhodnocovány?

H.35 Jsou zařízení pro zaznamenávání logů chráněna proti zfalšování a neoprávněnému přístupu?

H.36 Zaznamenáváte činnosti administrátora a operátorů?

H.37 Zaznamenáváte a analyzujete chyby?

H.38 Přijímáte u těchto chyb příslušná opatření?

H.39 Jsou hodiny všech příslušných systémů zpracovávajících informace v organizaci nebo bezpečnostní zóně synchronizovány podle odsouhlaseného zdroje času?

I Řízení přístupu

I.1 Jsou požadavky organizace na řízení přístupu vymezeny, dokumentovány a přezkoumány podle podnikových bezpečnostních požadavků na přístupy?

I.2 Existuje postup pro formální registraci uživatele včetně jejího zrušení, který zajistí propůjčení přístupu ke všem víceuživatelským informačním systémům a službám?

I.3 Existuje systém správy a postupy pro přidělování hesel?

I.4 Je přidělování hesel řízeno formalizovaným postupem?

I.5 Přezkoumává management v pravidelných intervalech přístupová práva uživatelů formalizovaným postupem?

I.6 Je na uživatelích vyžádáno, aby při výběru a použití hesel správně dodržovali bezpečnostní postupy?

I.7 Je na uživatelích vyžádáno, aby zajistili přiměřenou ochranu neobsluhovaných zařízení?

I.8 Je přijata a realizována politika čistého stolu nejen pro papíry, ale rovněž pro přenosná média a prázdné obrazovky u zařízení pro zpracování informací?

I.9 Smí mít uživatelé přímý přístup pouze ke službám, pro jejichž užití byli zvlášť oprávněni?

I.10 Je vzdálený přístup uživatelů předmětem zvláštních metod autentizace?

I.11 Využíváte jako prostředek prokázání autentického připojení ze specifických lokalit a zařízení automatické identifikace zařízení?

I.12 Je přístup k diagnostickým portům bezpečně řízen?

I.13 Jsou do sítí zavedena opatření pro oddělení skupin informačních služeb, uživatelů a informačních systémů?

I.14 Je ve sdílených sítích vymezena možnost připojení uživatelů v souladu s politikou řízení přístupu?

I.15 Jsou sdílené sítě vybaveny řízeným směrováním, které zajistí, že spojení počítačů a informační toky nejsou v rozporu s politikou řízení přístupu k aplikacím organizace?

I.16 Je přístup k operačním systémům řízen bezpečným postupem pro přihlašování?

I.17 Užívají všichni uživatelé při své činnosti jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti?

I.18 Máte zaveden systém správy hesel pro zajištění efektivního a interaktivního posouzení kvality hesel?

I.19 Je použití systémových programových nástrojů omezeno a přísně řízeno?

I.20 Jsou neaktivní terminály na vysoce rizikových místech nebo u vysoce rizikových systémů po předem určeném období nečinnosti odpojeny?

I.21 Je u vysoce rizikových aplikací omezena doba, kdy je možno se k nim připojit?

I.22 Je přístup uživatelů a podpůrných zaměstnanců k informacím a funkcím aplikačního systému omezen v souladu s politikou řízení přístupu?

I.23 Jsou citlivé systémy provozovány v odděleném prostředí?

I.24 Jsou v organizaci schváleny formální zásady a vhodná opatření pro ochranu před riziky, která plynou z práce na mobilních výpočetních prostředcích?

I.25 Je pro autorizaci a řízení práce na dálku vytvořena bezpečnostní politika a postupy?

J Sběr dat, vývoj a údržba informačních systémů

J.1 Jsou do požadavků organizace na nové informační systémy nebo na rozšíření systémů promítnuty požadavky na nové bezpečnostní opatření?

J.2 Jsou data vstupující do zpracování validována, aby byla zajištěna jejich správnost a vhodnost?

J.3 Je do aplikací pro detekci jakéhokoli porušení informací během interního zpracování vlivem chyb při zpracování informace nebo úmyslným zásahem začleněna validace informací?

J.4 Máte identifikovány požadavky na zajištění autentičnosti a ochranu neporušenosti zpráv z aplikací a identifikována a zavedena příslušná opatření?

J.5 Je datový výstup aplikačního systému kontrolován, aby bylo zajištěno, že zpracování uložených informací probíhá správně a je přiměřené okolnostem?

J.6 Máte vytvořenu a dodržovánu příslušnou politiku pro použití kryptografických kontrol, které jsou určeny k ochraně informací?

J.7 Je pro podporu kryptografických technik používán systém správy klíčů, který je založen na dohodnuté soustavě norem, postupů a metod?

J.8 Existují postupy pro řízené instalování programů do operačních systémů?

J.9 Jsou testovací data pečlivě volena, chráněna a kontrolována?

J.10 Je přístup do knihoven zdrojových kódů programů podroben přísným omezením?

J.11 Je implementace změn striktně řízena s využitím postupů formálního změnového řízení?

J.12 Jsou aplikace významné pro podnikání přezkoumávány a testovány se změnou operačních systémů, aby nemohlo dojít k nežádoucímu dopadu na podnikové operace nebo bezpečnost?

J.13 Jsou změny ve funkčnosti programového vybavení omezeny na nezbytně nutné změny?

J.14 Jsou tyto změny striktně řízeny?

J.15 Předcházíte možnosti úniku informací?

J.16 Je outsourcing vývoje programu pod dohledem a monitorován organizací?

J.17 Vyžadujete a získáváte aktuální informace o technických zranitelnostech informačních systémů?

J.18 Vyhodnocujete náchylnost systému v rámci organizace k těmto zranitelnostem a přijímáte vhodná opatření pro minimalizaci rizika?

K Řízení incidentů v oblasti bezpečnosti informací

K.1 Jakmile jsou zjištěny mimořádné události v rámci systému bezpečnosti informací, jsou vhodným služebním postupem co nejdříve hlášeny?

K.2 Vyžadujete, aby všichni zaměstnanci, smluvní dodavatelé a uživatelé informačních systémů a služeb z třetích stran zaznamenali a ohlásili jakékoliv pozorované nebo očekávané zranitelné místo v systému čí hrozbu pro systém?

K.3 Máte stanoveny odpovědnosti managementu a postupy pro zajištění rychlé, efektivní a systematické odezvy na informaci o bezpečnostním incidentu?

K.4 Máte zaveden mechanismus, umožňující kvantifikovat a monitorovat druhy, rozsah a související náklady ve vztahu vůči incidentům v rámci zajišťování bezpečnosti informací?

K.5 Jsou při následné akci proti osobám nebo organizaci po incidentu, jenž souvisí s porušením právních předpisů, shromážděny důkazy a uchovány a prezentovány podle předpisů, uvedených v příslušném právním předpise?

L Řízení kontinuity činností organizace

L.1 Existuje v rámci organizace řízený proces pro rozvoj a udržování kontinuity činností organizace, který pokrývá požadavky na bezpečnost informací, nezbytné pro zachování kontinuity podnikových procesů?

L.2 Jsou identifikovány události, které mohou způsobit přerušení podnikových procesů, včetně vyhodnocení pravděpodobnosti a dopadu takových přerušení a jejich důsledky na bezpečnost informací?

L.3 Máte připraveny a zavedeny plány pro udržování a obnovování činností pro případ přerušení nebo poruchu kritických firemních aktivit?

L.4 Obsahují tyto plány instrukce pro předepsané funkce včetně časové souslednosti?

L.5 Je udržována jednoduchá kostra plánů kontinuity činností organizace, která zajistí, že jsou všechny plány konzistentní, konzistentně pokrývají všechny požadavky na bezpečnost, a která určí priority pro testování a údržbu?

L.6 Jsou plány kontinuity pravidelně testovány a udržovány, aby se zajistilo, že jsou aktuální a efektivní?

M Soulad s požadavky

M.1 Jsou požadavky, vyplývající ze zákonů a ze smluv, pro každý informační systém a organizaci explicitně vymezeny, dokumentovány a udržovány v aktuálním stavu?

M.2 Máte zavedeny příslušné postupy pro zajištění shody se zákonnými nebo smlouvami vymezenými omezeními, vztahujícími se k užití materiálů a programového vybavení, které jsou předmětem práv duševního vlastnictví?

M.3 Jsou důležité doklady organizace chráněny před ztrátou, zničením a padělaním v souladu s požadavky zákonů, dalších předpisů, smluv a postupů v rámci vlastní organizace?

M.4 Je zajištěna ochrana osobních údajů v souladu se zákonnými požadavky a dalšími předpisy, a pokud je to potřebné i podle požadavků ze smluv?

M.5 Je v organizace zabráněno uživatelům, aby využívali zařízení v neautorizovaném režimu?

M.6 Jsou kryptografické prostředky používány v souladu s dohodami, zákonnými a jinými předpisy?

M.7 Zaručí vedoucí zaměstnanci, že všechny bezpečnostní postupy, které patří do jejich odpovědnosti, jsou prováděny správně?

M.8 Jsou všechny oblasti uvnitř organizace předmětem pravidelného ověření, které posoudí soulad s bezpečnostními politikami a normami bezpečnosti?

M.9 Je pravidelně ověřován soulad informačních systémů s normami pro implementaci bezpečnosti?

M.10 Jsou požadavky na audit a činnosti, související s kontrolou zajištění bezpečnosti, prováděné v rámci auditu přímo na pracovních systémech pečlivě plánovány a odsouhlaseny v rámci organizace, aby se minimalizovalo riziko přerušení podnikových procesů?

M.11 Je chráněn přístup k nástrojům auditu, aby bylo zabráněno jejich zneužití nebo ohrožení?

Pomocí vzorce (3.2) jsem u každého prvku systému bezpečnosti vypočetla jeho míru plnění (viz. tab. 3.5).

1	Politika bezpečnosti informací	80,0%
2	Organizace bezpečnosti informací	92,0%
3	Externí partneři	100,0%
4	Řízení aktiv	95,0%
5	Klasifikace informací	100,0%
6	Bezpečnost lidských zdrojů	89,1%
7	Fyzická bezpečnost a bezpečnost prostředí	89,3%
8	Řízení telekomunikace a řízení provozu	92,8%
9	Řízení přístupu	94,4%
10	Sběr dat, vývoj a údržba informačních systémů	91,8%
11	Řízení incidentů v oblasti bezpečnosti informací	92,0%
12	Řízení kontinuity činností organizace	83,3%
13	Soulad s požadavky	98,2%

Tab. 3.5 Míra plnění jednotlivých prvků systému bezpečnosti

Do vzorce (3.3) jsem dosadila sumu míry plnění všech prvků ISMS a vydělila ji celkovým počtem prvků, které byly hodnoceny. Souhrnné hodnocení bezpečnosti informací ve firmě Doprava s.r.o je podle normy ISO/IEC 27000 92,1%.

$$H = \frac{\text{Suma míry plnění hodnocené kapitoly ISMS}}{\text{Počet hodnocených kapitol (prvků) ISMS}} = \frac{1197,9\%}{13} = \mathbf{92,1\%}$$

Souhrnná míra plnění v %	Hodnocení ISMS
90 – 100	Vyhověl
80 – 89,99	Převážně vyhovující
60 – 79,99	Podmíněně vyhovující
Méně než 60	Nevyhovující

Tab. 3.6 Hodnocení ISMS

Zdroj: DRASTICH, M. Bezpečnost a ochrana dat a informací. 96 s.

Podle tab. 3.6 firma Doprava s.r.o. vyhověla podmínkám auditu a její systém zabezpečení je vhodný pro její další vývoj a uplatnění na trhu. Audit IT nedošel k vážnějším prohřeškům proti hodnotící normě.

3.3 Shrnutí

Z míry plnění vyplývá, že nejhůře hodnoceným prvkem systému bezpečnosti je politika bezpečnosti informací a nejlépe hodnocená kapitola je klasifikace informací a externí partneři.

Následující přehled vypovídá o hlavních nedostatcích jednotlivých kapitol ISMS a tento přehled je doplněn o návrh řešení těchto nedostatků v souladu s možnostmi firmy Doprava s.r.o.

a) Politika bezpečnosti informací:

- × Nedostatek: Dokument bezpečnosti informací není vhodným způsobem sdělen partnerům firmy Doprava s.r.o.
- ✓ Návrh řešení: Provést analýzu potřeby informovanosti partnera v souvislosti se zajištěním bezpečnosti informací.

b) Organizace bezpečnosti:

- × Nedostatek: Společnost neudržuje kontakty se všemi potřebnými odbornými skupinami.
- ✓ Návrh řešení: Vytvořit tým odborníků, který by nastavil potřebné informační procesy.

c) Bezpečnost lidských zdrojů:

- × Nedostatek: Kontrola a přezkoumání předchozích činností všech kandidátů na zaměstnání neprobíhají v plném rozsahu.
- ✓ Návrh řešení: Provést analýzu pracovních pozic a označit pozice, pro které je nutné ověření jejich předchozí činnosti s ohledem na bezpečnost informací.
- × Nedostatek: Disciplinární proces pro zaměstnance, kteří ohrozili bezpečnost firmy, není formalizován.
- ✓ Návrh řešení: Pověřit personální odbor společnosti zpracováním řídícího dokumentu pro řešení požadovaného úkolu.

d) Fyzická bezpečnost:

- × Nedostatek: Bezpečnost kabeláže není zcela zajištěna a zdokumentována.
- ✓ Návrh řešení: Oslovit externí společnost s úkolem zajistit informační síť proti úniku informací.
- × Nedostatek: U zařízení, které je použito mimo objekty organizace, nejsou zohledněna všechna rizika s tím spojená.
- ✓ Návrh řešení: U nechráněných přístrojů nezpracovávat citlivé informace.

e) Řízení telekomunikace a řízení provozu:

- × Nedostatek: Povinnosti nejsou zcela odděleny od oblastí odpovědnosti.
- ✓ Návrh řešení: Provést analýzu principu čtyř očí[1] a zhodnotit výši nebezpečí zneužití informací.
- × Nedostatek: Chybí dokumentace k politikám, postupům a opatřením pro ochranu výměny informací s použitím všech typů telekomunikačních zařízení.
- ✓ Návrh řešení: Zajistit dokumentaci odpovědným pracovníkem.

f) Řízení přístupu:

- × Nedostatek: U vysoce rizikových aplikací není omezena doba, kdy je možno se k nim připojit.

[1] „princip čtyř očí“ – kontrolní činnosti, odpovědnosti a povinnosti, které vedou k neomezenému přístupu k systému, nesmí být vykonávány jedinou osobou

- Vyhodnocení: Společnost zajišťuje nepřetržitý provoz a z toho důvodu nelze časově omezit práci systému.

g) Sběr dat, vývoj a údržba informačních systémů:

   × Nedostatek: Do aplikací pro detekci porušení informací během interního zpracování není začleněna validace informací.

   ✓ Návrh řešení: Společnost by měla zpracovat projekt pro zajištění nápravy.

h) Řízení incidentů v oblasti bezpečnosti informací:

   × Nedostatek: Společnost nemá zdokumentován mechanismus umožňující kvantifikovat a monitorovat druhy, rozsah a související náklady ve vztahu vůči incidentům.

   ✓ Návrh řešení: Zajištění dokumentace odpovědnou osobou.

i) Řízení kontinuity činností organizace:

   × Nedostatek: Plány kontinuity společnosti nejsou zcela zdokumentovány a pravidelnost jejich testování není vždy dodržena.

   ✓ Návrh řešení: Pro zajištění uvedených úkolů by měly být ve společnosti nastaveny reporty vedoucím pracovníkům a plnění těchto úkolů by mělo být zahrnuto do klíčových ukazatelů vedoucích pracovníků.

Kapitoly externí partneři, řízení aktiv, klasifikace informací a soulad s požadavky se vážněji neodchylují od požadavků normy ISO/IEC 27000.

Závěr

Bezpečnost informací je nedílnou součástí chodu každé úspěšné firmy. Je třeba si uvědomit, jakou důležitost mají data pro jednotlivé organizace. Ať se jedná o údaje zákazníků, nebo statistická data, jejich ztráta se projeví na chodu firmy a v horších případech i na jejím renomé.

Audit IT by měl těmto incidentům předcházet a upozornit na oblasti v ISMS, které nesplňují podmínky bezpečnosti a narušují tak zabezpečení celé společnosti.

Cílem této práce bylo prověřit zabezpečení firmy Doprava s.r.o. pomocí standardu, který by vyhovoval potřebám a požadavkům této společnosti. K tomuto účelu byla nakonec vybrána norma ISO/IEC 27000, která prověřuje komplexní systém zabezpečení a v posledních letech se uplatňuje jako účinný prostředek ochrany proti bezpečnostním incidentům, což se projevuje i jejím nástupem v oblasti zabezpečení firem v České republice (viz. obr. 2.4). Cílem této normy je sjednotit požadavky, návody a doporučení na systémy řízení informační bezpečnosti, které se vyskytují v různých normách.

Bezpečnost informací firmy Doprava s.r.o. byla shledána jako vyhovující a k jednotlivým nedostatkům kapitol ISMS, které byly zjištěny v průběhu auditu, byl vypracován návrh jejich řešení. Firma Doprava s.r.o. byla spravena o výsledcích auditu a nepodala žádné námitky ani připomínky k průběhu auditu ani k jeho výsledkům.

Seznam použité literatury:

a) tištěné publikace:

[1] ČSN EN ISO 19011. *Směrnice pro auditování systému managementu jakosti a/nebo systému enviromentálního managementu*. Praha : Český normalizační institut, 2003. 56 s.

[2] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky : Systémy managementu bezpečnosti informací – Požadavky*. Praha : Český normalizační institut, 2006. 36 s.

[3] ČSN ISO/IEC 17799. *Informační technologie – Bezpečnostní techniky : Soubor postupů pro management bezpečnosti informací*. Praha : Český normalizační institut, 2006. 102 s.

[4] DRASTICH, M. *Bezpečnost a ochrana dat a informací : doktorská disertační práce.* Ostrava : VŠB – Technická univerzita Ostrava, Ekonomická fakulta, 2007. 96 s.

[5] ŠEBESTA, V., ŠTVERKA, V., STEINER, F., ŠEBESTOVÁ, M. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. 1. vyd. Český normalizační institut, 2006. 70 s. ISBN 80-7283-204-2.

b) elektronické zdroje:

[6] ADÁMEK, Martin. Kvalitativní standardy v IS/ICT : Koncept ITIL. *Moderní řízení* [online]. 2006, roč. 6, č. 9 [cit. 2008-02-24]. Dostupný z WWW: <http://modernirizeni.ihned.cz/c4-10065470-19237620-600000_d-kvalitativni-standardy-v-is-ict-cast-3-koncept-itil>.

[7] ADÁMEK, Martin. Kvalitativní standardy v IS/ICT : COBIT a IT Service Management. *Moderní řízení* [online]. 2006, roč. 6, č. 8 [cit. 2008-03-12]. Dostupný z WWW: <http://modernirizeni.ihned.cz/2-19058910-600000_d-8c>.

[8] HUJŇÁK, Petr. *IT Governance : Řízení a správa informatiky v podmínkách SME* [online]. Per Partes Consulting, [2005] [cit. 2008-03-29]. Dostupný z WWW: <http://www.cacio.cz/data/sharedfiles/Sborniky/sbor-aspekty-1-hujnak-01.pdf>.

Seznam zkratek a symbolů

IS – informační systém

ISMS – systém managementu bezpečnosti informací

IS/ICT – informační systémy a informační a komunikační technologie

IT – informační technologie

ISO – mezinárodní organizace pro normalizaci

IEC – mezinárodní elektrotechnická komise

ITIL – knihovna infrastruktury informačních technologií

COBIT – kontrolní rámec pro řízení informačních technologií

SW – software

MS – míra splnění

MO – míra ověření

H – hodnocení

H_m – maximální hodnocení

NR – tato otázka není relevantní

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- byla jsem seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo,
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně ke své vnitřní potřebě bakalářskou práci užít (§ 35 odst. 3),
- souhlasím s tím, že jeden výtisk bakalářské práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o bakalářské práci, obsažené v Záznamu o závěrečné práci, umístěném v příloze mé bakalářské práce, budou zveřejněny v informačním systému VŠB-TUO,
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona,
- bylo sjednáno, že užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……..

……..
Jiřina Petříková

Adresa trvalého pobytu studenta:
U Lesa 701
Vřesina
742 85

Seznam příloh:

Příloha č. 1: Otázky k auditu informační bezpečnosti (tabulka)

Příloha č. 2: Přehled míry plnění jednotlivých prvků ISMS (graf)

Příloha č. 1: Otázky k auditu informační bezpečnosti (tabulka)

	Otázky k auditu bezpečnosti	MS	MO	H	H_m
A	***Politika bezpečnosti informací***				
A.1	Máte dokument politiky bezpečnosti informací schválen vedoucími zaměstnanci?	A	A	10	**10**
A.2	Je zveřejněn a sdělen všem zaměstnancům?	A	A	10	**10**
A.3	Je sdělen partnerům?	B	C	2	**10**
A.4	Je politika bezpečnosti informací revidována v pravidelných intervalech a v případě podstatných změn pro zajištění kontinuální vhodnosti, přiměřenosti a účinnosti?	A	A	10	**10**
	Suma			32	**40**
	Míra plnění			**80%**	
B	***Organizace bezpečnosti informací***				
B.1	Podporuje vedení aktivně bezpečnost informací?	A	A	10	**10**
B.2	Vyjádřilo vedení jasně svůj závazek a potvrdilo odpovědnost za bezpečnost informací?	A	A	10	**10**
B.3	Jsou aktivity pro zajištění bezpečnosti informací koordinovány představiteli z různých částí organizace?	A	A	10	**10**
B.4	Jsou určeny odpovědnosti za ochranu jednotlivých aktiv a za realizaci určených bezpečnostních procesů?	A	A	10	**10**
B.5	Máte určen postup schvalování nových prostředků pro zpracování informací z pozice managementu?	A	A	10	**10**
B.6	Máte identifikovány požadavky na důvěrnost nebo dohody o neprozrazení reflektující potřeby organizace ochránit své informace?	A	A	10	**10**
B.7	Jsou tato ujednání pravidelně přezkoumávána?	A	B	8	**10**
B.8	Udržujete příslušné kontakty s odpovídajícími autoritami (např. orgány státní správy)?	A	A	10	**10**
B.9	Udržujete příslušné kontakty s příslušnými zainteresovanými odbornými skupinami nebo jinými specializovanými bezpečnostními fóry a profesními sdruženími?	B	B	4	**10**
B.10	Přezkoumáváte přístup organizace k řízení bezpečnosti informací a jeho zavedení v pravidelných intervalech a při významných změnách, které mohou ovlivnit bezpečnost (tzn. cíle řízení, opatření, politiky, procesy a všechny postupy pro bezpečnost informací)?	A	A	10	**10**
	Suma			92	**100**
	Míra plnění			**92%**	
C	***Externí partneři***				
C.1	Máte identifikována rizika, spojená s informacemi a zařízeními, fungujícími v rámci nakládání s informacemi, vznikající v procesech chodu podniku, do kterých jsou zapojeny třetí strany?	A	A	10	**10**

C.2	Máte přijata příslušná opatření ještě před udělením přístupových práv?	A	A	10	**10**
C.3	Zvažujete všechny identifikované bezpečnostní požadavky před zpřístupněním informačních aktiv nebo informací zákazníkovi?	A	A	10	**10**
C.4	Zohledňují smlouvy se třetími stranami, obsahující přístupy, činnosti, komunikování nebo řízení informací organizace nebo jejího zařízení pro nakládání s informacemi všechny příslušné požadavky na bezpečnost?	A	A	10	**10**
C.5	Zohledňují tyto požadavky také doplňující produkty nebo služby k zařízením pro zpracování informací?	NR		NR	
	Suma			40	**40**
	Míra plnění			**100%**	
D	***Řízení aktiv***				
20	Máte zavedenu evidenci všech důležitých aktiv spojených s informačními systémy?	A	A	10	**10**
21	Je tato evidence udržována?	A	A	10	**10**
22	Jsou všechny informace a aktiva spojená se zařízeními pro zpracování informací ve vlastnictví přesně označeného útvaru organizace?	A	A	10	**10**
23	Máte identifikována, dokumentována a zavedena pravidla pro přijatelné využívání informací a aktiv spojených se zařízením pro zpracování informací?	A	B	8	**10**
	Suma			38	**40**
	Míra plnění			**95%**	
E	***Klasifikace informací***				
E.1	Jsou informace v organizaci klasifikovány podle svého významu, právních požadavků, citlivosti a významnosti pro organizaci?	A	A	10	**10**
E.2	Máte vymezen pro označování a zpracování informací přiměřený soubor postupů, které jsou ve shodě s klasifikačním schématem přijatým organizací?	A	A	10	**10**
	Suma			20	**20**
	Míra plnění			**100%**	
F	***Bezpečnost lidských zdrojů***				
F.1	Máte stanoveny a dokumentovány bezpečnostní úlohy a odpovědnosti zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran v souladu s politikou bezpečnosti informací organizace?	A	A	10	**10**
F.2	Provádíte kontrolu a přezkoumání předchozích činností všech kandidátů na zaměstnání, smluvních dodavatelů a uživatelů z třetích stran podle příslušných zákonů a pravidel a úměrně požadavkům podniku?	B	A	6	**10**
F.3	Provádíte tuto kontrolu úměrně klasifikaci informací, se kterými mají nakládat a s nimi spojených rizik?	A	A	10	**10**

F.4	Musí zaměstnanci, smluvní dodavatelé a uživatelé z třetí strany při uzavírání pracovní smlouvy odsouhlasit a podepsat ustanovení týkající se odpovědnosti za bezpečnost informací jako součást svých podmínek pracovního poměru v pracovní smlouvě?	A	A	10	**10**
F.5	Vyžaduje management, aby zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran dodržovali bezpečnost podle vyhlášených politik a postupů organizace?	A	A	10	**10**
F.6	Musí zaměstnanci organizace, a je-li to důležité, i uživatelé třetích stran absolvovat odpovídající, pravidelně se opakující školení, vztahující se k politice bezpečnosti informací a postupům organizace?	A	A	10	**10**
F.7	Máte zaveden formalizovaný disciplinární proces pro zaměstnance, kteří ohrozili bezpečnostní rozhraní?	A	C	6	**10**
F.8	Máte jasně určeny a formulovány odpovědnosti při ukončování zaměstnaneckého poměru nebo při změně zaměstnání v rámci organizace?	A	A	10	**10**
F.9	Musí zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran před ukončením zaměstnání, smlouvy nebo dohody vrátit všechna aktiva, náležející organizaci, která spravovali při výkonu funkce?	A	A	10	**10**
F.10	Jsou přístupová práva všech zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran k informacím a zařízením pro zpracování informací odejmuta před ukončením jejich zaměstnanosti, smlouvy nebo dohody?	A	A	10	**10**
F.11	Jsou přístupová práva v případě změny včas aktualizována podle povahy změny?	B	A	6	**10**
	Suma			98	**110**
	Míra plnění			**89%**	
G	***Fyzická bezpečnost a bezpečnost prostředí***				
G.1	Používáte při ochraně prostor, ve kterých se nachází zařízení pro zpracování informací, bezpečnostní perimetry (bariéry jako zdi, vstupy pomocí čipových karet, recepce apod.)?	A	A	10	**10**
G.2	Jsou bezpečné prostory chráněny vhodnými opatřeními, aby byl přístup povolen pouze oprávněným osobám?	A	A	10	**10**
G.3	Jsou vytvořeny zabezpečené oblasti pro ochranu kanceláří, místností a vybavení se zvláštními bezpečnostními požadavky?	A	A	10	**10**
G.4	Máte zavedenu fyzickou ochranu proti zničení požárem, povodní, zemětřesením, explozí a dalším živelným nebo společenským ohrožením?	A	A	10	**10**
G.5	Využíváte další opatření a směrnice pro zvýšení bezpečnosti v zabezpečených oblastech?	A	A	10	**10**
G.6	Máte pod dohledem přístupová místa, díky kterým by neautorizované osoby mohly vstoupit do prostorů organizace?	A	A	10	**10**
G.7	Pokud je to možné, jsou tato místa izolována od zařízení pro zpracování informací, aby nemohlo dojít k neautorizovanému přístupu?	A	B	8	**10**

G.8	Máte všechna zařízení umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím?	A	A	10	**10**
G.9	Máte bezpečnostní opatření k omezení příležitosti pro neoprávněný přístup k zařízením?	A	A	10	**10**
G.10	Jsou tato zařízení chráněna před selháním napájení a před dalšími formami přerušení, způsobenými poruchami podpůrných zařízení?	A	A	10	**10**
G.11	Je silová a telekomunikační kabeláž, určená pro přenos dat a podporu informačních služeb, chráněna před poškozením či odposlechem?	B	C	2	**10**
G.12	Jsou veškerá zařízení udržována v souladu s pokyny výrobce a s dokumentovanými postupy?	A	B	8	**10**
G.13	Jsou při ochraně zařízení, které je použito mimo objekty organizace, zohledněna různá rizika prací mimo prostory organizace?	B	A	6	**10**
G.14	Jsou všechny prvky zařízení, obsahujícího paměťová média, před tím, než se dají dále k dispozici, zkontrolovány, aby se zajistilo odstranění všech citlivých dat a softwarů?	A	A	10	**10**
G.15	Je možno odstranit vybavení, informace a software jen se schválením (autorizací)?	A	A	10	**10**
	Suma			134	**150**
	Míra plnění			**89%**	
H	***Řízení telekomunikace a řízení provozu***				
H.1	Jsou provozní postupy dokumentovány, udržovány a k dispozici všem, kteří je potřebují?	A	B	8	**10**
H.2	Provádí se změny na zařízeních, využívaných pro práci s informacemi, řízeným způsobem?	A	A	10	**10**
H.3	Jsou povinnosti odděleny od oblastí odpovědnosti, aby se omezila příležitost neoprávněné nebo i neúmyslné modifikace nebo zneužití aktiv organizace?	B	B	4	**10**
H.4	Je od sebe odděleno vybavení pro vývoj, testování a provoz, aby se snížilo riziko neautorizovaného přístupu nebo změn v operačním systému?	A	A	10	**10**
H.5	Máte zajištěno, aby smlouvy se třetí stranou o dodávání služeb obsahovaly výčet opatření, přesná stanovení služeb a úrovně jejich dodávání?	A	A	10	**10**
H.6	Obsahují tyto smlouvy požadavek, aby třetí strany tato ustanovení průkazně dodržovaly?	A	A	10	**10**
H.7	Jsou služby, hlášení o jejich provádění a záznamy poskytované třetí straně pravidelně monitorovány a přezkoumávány (včetně pravidelného provádění auditů)?	A	A	10	**10**
H.8	Jsou změny v rámci poskytovaných služeb, včetně udržování a zlepšování existujících informačních politik, postupů a opatření řízeny?	A	A	10	**10**
H.9	Je v rámci provádění změn provedeno nové hodnocení rizik?	A	A	10	**10**

H.10	Je využívání zdrojů monitorováno a vylaďováno pro zajištění požadované výkonnosti systému?	A	A	10	**10**
H.11	Děláte prognózy požadavků na budoucí kapacity?	A	A	10	**10**
H.12	Máte určena kritéria pro akceptaci nových systémů, jejich aktualizaci a zavádění nových verzí?	A	A	10	**10**
H.13	Jsou tato kritéria podpořena vhodnými testy systému, které jsou prováděny před vlastní akceptací?	A	A	10	**10**
H.14	Máte implementována opatření pro odhalování, prevenci a znovunabytí ztracených dat, aby byla zajištěna ochrana před působením škodlivých programů a aby bylo zvyšováno odpovídající bezpečnostní povědomí uživatelů?	A	B	8	**10**
H.15	Máte zajištěno pomocí správného nastavení konfigurace, aby autorizovaný mobilní kód pracoval v souladu s jasně stanovenou bezpečnostní politikou a aby fungovala ochrana proti využívání neautorizovaného kódu? (Jen pokud je v organizaci povoleno využívání mobilních kódů)	NR		NR	
H.16	Pořizujete pravidelně záložní kopie informací a programového vybavení podle odsouhlasené politiky pro zálohování?	A	A	10	**10**
H.17	Jsou tyto kopie pravidelně testovány?	A	A	10	**10**
H.18	Jsou sítě v organizaci přiměřeně kontrolovány a řízeny?	A	A	10	**10**
H.19	Jsou zvláštní požadavky na bezpečnost, úrovně služeb a požadavky na management všech síťových služeb správně identifikovány a zavedeny do všech smluv na síťové služby?	A	B	8	**10**
H.20	Existují postupy pro správu vyměnitelných počítačových médií?	A	A	10	**10**
H.21	Jsou média, která jsou dále provozně neupotřebitelná, bezpečně a spolehlivě zlikvidována dokladovanými postupy?	A	A	10	**10**
H.22	Jsou vytvořeny postupy pro nakládání s informacemi a jejich ukládání, které je chrání před neoprávněným využitím nebo prozrazením?	A	A	10	**10**
H.23	Je systémová dokumentace chráněna před neoprávněným přístupem?	A	A	10	**10**
H.24	Existují politiky, postupy a opatření pro ochranu výměny informací s použitím všech typů komunikačních zařízení?	A	C	6	**10**
H.25	Jsou mezi organizací a externími partnery uzavřeny dohody pro výměnu informací a programového vybavení?	A	A	10	**10**
H.26	Jsou média obsahující informace chráněna proti neautorizovanému přístupu, zneužití nebo poškození při transportu mimo organizaci?	A	A	10	**10**
H.27	Jsou informace přenášené elektronickou poštou vhodným způsobem chráněny?	A	A	10	**10**
H.28	Jsou vytvořeny a zavedeny politiky a postupy pro ochranu informací souvisejících s propojením obchodních informačních systémů?	A	A	10	**10**
H.29	Jsou informace z elektronického obchodování, které procházejí přes veřejné sítě, ochráněny od podvodných aktivit, nedorozumění ve smlouvách a neoprávněných odhaleních a modifikacích?	NR		NR	

H.30	Jsou informace týkající se obchodů uzavíraných on-line chráněny, aby se zabránilo neúplnému přenosu, chybnému směrování, neoprávněné úpravě, neoprávněnému odhalení, neoprávněnému zdvojení nebo modifikaci?	NR		NR	
H.31	Je chráněna celistvost informací, které jsou k dispozici na veřejně přístupných systémech, aby nemohlo dojít k neoprávněné modifikaci?	A	A	10	**10**
H.32	Jsou auditní logy, zaznamenávající aktivity uživatelů, výjimky a události související s bezpečností informací udržovány po stanovenou dobu pro účely možných budoucích vyšetřování a monitorování řízení přístupů?	A	A	10	**10**
H.33	Máte určeny postupy pro monitorování využití zařízení pro zpracování informací?	A	A	10	**10**
H.34	Jsou výsledky z těchto zařízení pravidelně vyhodnocovány?	B	C	2	**10**
H.35	Jsou zařízení pro zaznamenávání logů chráněna proti zfalšování a neoprávněnému přístupu?	A	A	10	**10**
H.36	Zaznamenáváte činnosti administrátora a operátorů?	A	B	8	**10**
H.37	Zaznamenáváte a analyzujete chyby?	A	A	10	**10**
H.38	Přijímáte u těchto chyb příslušná opatření?	A	A	10	**10**
H.39	Jsou hodiny všech příslušných systémů zpracovávajících informace v organizaci nebo bezpečnostní zóně synchronizovány podle odsouhlaseného zdroje času?	A	A	10	**10**
	Suma			334	**360**
	Míra plnění			**93%**	
I	***Řízení přístupu***				
I.1	Jsou požadavky organizace na řízení přístupu vymezeny, dokumentovány a přezkoumány podle podnikových bezpečnostních požadavků na přístupy?	A	A	10	**10**
I.2	Existuje postup pro formální registraci uživatele včetně jejího zrušení, který zajistí propůjčení přístupu ke všem víceuživatelským informačním systémům a službám?	A	A	10	**10**
I.3	Existuje systém správy a postupy pro přidělování hesel?	A	A	10	**10**
I.4	Je přidělování hesel řízeno formalizovaným postupem?	A	A	10	**10**
I.5	Přezkoumává management v pravidelných intervalech přístupová práva uživatelů formalizovaným postupem?	A	A	10	**10**
I.6	Je na uživatelích vyžádáno, aby při výběru a použití hesel správně dodržovali bezpečnostní postupy?	A	A	10	**10**
I.7	Je na uživatelích vyžádáno, aby zajistili přiměřenou ochranu neobsluhovaných zařízení?	A	A	10	**10**
I.8	Je přijata a realizována politika čistého stolu nejen pro papíry, ale rovněž pro přenosná média a prázdné obrazovky u zařízení pro zpracování informací?	A	A	10	**10**
I.9	Smí mít uživatelé přímý přístup pouze ke službám, pro jejichž užití byli zvlášť oprávněni?	A	A	10	**10**

I.10	Je vzdálený přístup uživatelů předmětem zvláštních metod autentizace?	A	A	10	**10**
I.11	Využíváte jako prostředek prokázání autentického připojení ze specifických lokalit a zařízení automatické identifikace zařízení?	A	A	10	**10**
I.12	Je přístup k diagnostickým portům bezpečně řízen?	A	B	8	**10**
I.13	Jsou do sítí zavedena opatření pro oddělení skupin informačních služeb, uživatelů a informačních systémů?	A	A	10	**10**
I.14	Je ve sdílených sítích vymezena možnost připojení uživatelů v souladu s politikou řízení přístupu?	A	A	10	**10**
I.15	Jsou sdílené sítě vybaveny řízeným směrováním, které zajistí, že spojení počítačů a informační toky nejsou v rozporu s politikou řízení přístupu k aplikacím organizace?	A	A	10	**10**
I.16	Je přístup k operačním systémům řízen bezpečným postupem pro přihlašování?	A	A	10	**10**
I.17	Užívají všichni uživatelé při své činnosti jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti?	A	A	10	**10**
I.18	Máte zaveden systém správy hesel pro zajištění efektivního a interaktivního posouzení kvality hesel?	A	A	10	**10**
I.19	Je použití systémových programových nástrojů omezeno a přísně řízeno?	A	A	10	**10**
I.20	Jsou neaktivní terminály na vysoce rizikových místech nebo u vysoce rizikových systémů po předem určeném období nečinnosti odpojeny?	A	A	10	**10**
I.21	Je u vysoce rizikových aplikací omezena doba, kdy je možno se k nim připojit?	C	C	0	**10**
I.22	Je přístup uživatelů a podpůrných zaměstnanců k informacím a funkcím aplikačního systému omezen v souladu s politikou řízení přístupu?	A	A	10	**10**
I.23	Jsou citlivé systémy provozovány v odděleném prostředí?	A	B	8	**10**
I.24	Jsou v organizaci schváleny formální zásady a vhodná opatření pro ochranu před riziky, která plynou z práce na mobilních výpočetních prostředcích?	A	A	10	**10**
I.25	Je pro autorizaci a řízení práce na dálku vytvořena bezpečnostní politika a postupy?	A	A	10	**10**
	Suma			236	**250**
	Míra plnění			**94%**	
J	***Sběr dat, vývoj a údržba informačních systémů***				
J.1	Jsou do požadavků organizace na nové informační systémy nebo na rozšíření systémů promítnuty požadavky na nové bezpečnostní opatření?	A	B	8	**10**
J.2	Jsou data vstupující do zpracování validována, aby byla zajištěna jejich správnost a vhodnost?	A	A	10	**10**

J.3	Je do aplikací pro detekci jakéhokoli porušení informací během interního zpracování vlivem chyb při zpracování informace nebo úmyslným zásahem začleněna validace informací?	C	C	0	**10**
J.4	Máte identifikovány požadavky na zajištění autentičnosti a ochranu neporušenosti zpráv z aplikací a identifikována a zavedena příslušná opatření?	A	A	10	**10**
J.5	Je datový výstup aplikačního systému kontrolován, aby bylo zajištěno, že zpracování uložených informací probíhá správně a je přiměřené okolnostem?	A	B	8	**10**
J.6	Máte vytvořenu a dodržovánu příslušnou politiku pro použití kryptografických kontrol, které jsou určeny k ochraně informací?	A	A	10	**10**
J.7	Je pro podporu kryptografických technik používán systém správy klíčů, který je založen na dohodnuté soustavě norem, postupů a metod?	A	A	10	**10**
J.8	Existují postupy pro řízené instalování programů do operačních systémů?	A	A	10	**10**
J.9	Jsou testovací data pečlivě volena, chráněna a kontrolována?	A	A	10	**10**
J.10	Je přístup do knihoven zdrojových kódů programů podroben přísným omezením?	A	A	10	**10**
J.11	Je implementace změn striktně řízena s využitím postupů formálního změnového řízení?	A	A	10	**10**
J.12	Jsou aplikace významné pro podnikání přezkoumávány a testovány se změnou operačních systémů, aby nemohlo dojít k nežádoucímu dopadu na podnikové operace nebo bezpečnost?	A	A	10	**10**
J.13	Jsou změny ve funkčnosti programového vybavení omezeny na nezbytně nutné změny?	A	A	10	**10**
J.14	Jsou tyto změny striktně řízeny?	A	A	10	**10**
J.15	Předcházíte možnosti úniku informací?	A	A	10	**10**
J.16	Je outsourcing vývoje programu pod dohledem a monitorován organizací?	NR		NR	
J.17	Vyžadujete a získáváte aktuální informace o technických zranitelnostech informačních systémů?	A	A	10	**10**
J.18	Vyhodnocujete náchylnost systému v rámci organizace k těmto zranitelnostem a přijímáte vhodná opatření pro minimalizaci rizika?	A	A	10	**10**
	Suma			156	**170**
	Míra plnění			**92%**	
K	***Řízení incidentů v oblasti bezpečnosti informací***				
K.1	Jakmile jsou zjištěny mimořádné události v rámci systému bezpečnosti informací, jsou vhodným služebním postupem co nejdříve hlášeny?	A	A	10	**10**
K.2	Vyžadujete, aby všichni zaměstnanci, smluvní dodavatelé a uživatelé informačních systémů a služeb z třetích stran zaznamenali a ohlásili jakékoliv pozorované nebo očekávané zranitelné místo v systému čí hrozbu pro systém?	A	A	10	**10**

K.3	Máte stanoveny odpovědnosti managementu a postupy pro zajištění rychlé, efektivní a systematické odezvy na informaci o bezpečnostním incidentu?	A	A	10	**10**
K.4	Máte zaveden mechanismus, umožňující kvantifikovat a monitorovat druhy, rozsah a související náklady ve vztahu vůči incidentům v rámci zajišťování bezpečnosti informací?	A	C	6	**10**
K.5	Jsou při následné akci proti osobám nebo organizaci po incidentu, jenž souvisí s porušením právních předpisů, shromážděny důkazy a uchovány a prezentovány podle předpisů, uvedených v příslušném právním předpise?	A	A	10	**10**
	Suma			46	**50**
	Míra plnění			**92%**	
L	***Řízení kontinuity činností organizace***				
L.1	Existuje v rámci organizace řízený proces pro rozvoj a udržování kontinuity činností organizace, který pokrývá požadavky na bezpečnost informací, nezbytné pro zachování kontinuity podnikových procesů?	A	B	8	**10**
L.2	Jsou identifikovány události, které mohou způsobit přerušení podnikových procesů, včetně vyhodnocení pravděpodobnosti a dopadu takových přerušení a jejich důsledky na bezpečnost informací?	A	A	10	**10**
L.3	Máte připraveny a zavedeny plány pro udržování a obnovování činností pro případ přerušení nebo poruchu kritických firemních aktivit?	A	A	10	**10**
L.4	Obsahují tyto plány instrukce pro předepsané funkce včetně časové souslednosti?	A	A	10	**10**
L.5	Je udržována jednoduchá kostra plánů kontinuity činností organizace, která zajistí, že jsou všechny plány konzistentní, konzistentně pokrývají všechny požadavky na bezpečnost, a která určí priority pro testování a údržbu?	A	B	8	**10**
L.6	Jsou plány kontinuity pravidelně testovány a udržovány, aby se zajistilo, že jsou aktuální a efektivní?	B	B	4	**10**
	Suma			50	**60**
	Míra plnění			**83%**	
M	***Soulad s požadavky***				
M.1	Jsou požadavky, vyplývající ze zákonů a ze smluv, pro každý informační systém a organizaci explicitně vymezeny, dokumentovány a udržovány v aktuálním stavu?	A	A	10	**10**
M.2	Máte zavedeny příslušné postupy pro zajištění shody se zákonnými nebo smlouvami vymezenými omezeními, vztahujícími se k užití materiálů a programového vybavení, které jsou předmětem práv duševního vlastnictví?	A	A	10	**10**
M.3	Jsou důležité doklady organizace chráněny před ztrátou, zničením a padělaním v souladu s požadavky zákonů, dalších předpisů, smluv a postupů v rámci vlastní organizace?	A	A	10	**10**

M.4	Je zajištěna ochrana osobních údajů v souladu se zákonnými požadavky a dalšími předpisy, a pokud je to potřebné i podle požadavků ze smluv?	A	A	10	**10**
M.5	Je v organizace zabráněno uživatelům, aby využívali zařízení v neautorizovaném režimu?	A	A	10	**10**
M.6	Jsou kryptografické prostředky používány v souladu s dohodami, zákonnými a jinými předpisy?	A	A	10	**10**
M.7	Zaručí vedoucí zaměstnanci, že všechny bezpečnostní postupy, které patří do jejich odpovědnosti, jsou prováděny správně?	A	B	8	**10**
M.8	Jsou všechny oblasti uvnitř organizace předmětem pravidelného ověření, které posoudí soulad s bezpečnostními politikami a normami bezpečnosti?	A	A	10	**10**
M.9	Je pravidelně ověřován soulad informačních systémů s normami pro implementaci bezpečnosti?	A	A	10	**10**
M.10	Jsou požadavky na audit a činnosti, související s kontrolou zajištění bezpečnosti, prováděné v rámci auditu přímo na pracovních systémech pečlivě plánovány a odsouhlaseny v rámci organizace, aby se minimalizovalo riziko přerušení podnikových procesů?	A	A	10	**10**
M.11	Je chráněn přístup k nástrojům auditu, aby bylo zabráněno jejich zneužití nebo ohrožení?	A	A	10	**10**
	Suma			108	**110**
	Míra plnění			**98%**	

Příloha č. 2: Přehled míry plnění jednotlivých prvků ISMS (graf)